Le nouveau dispositif de surveillance du net prêt à entrer en vigueur

PAR JÉRÔME HOURDEAUX
ARTICLE PUBLIÉ LE MERCREDI 31 DÉCEMBRE 2014

La veille de Noël, le gouvernement a publié le décret d'application de l'article 20 de la loi de programmation militaire votée il y a un an. Ce texte étend, les interceptions de communication sur internet et notamment la collecte des *« données de connexion »*. Il est critiqué par la CNIL et la CNCIS, la commission chargée de contrôler les interceptions de sûreté.

Le gouvernement a publié, à la veille de la fête de Noël, **le décret d'application** du controversé article 20 de la loi de programmation militaire (LPM) adoptée il y a un an et visant à renforcer la surveillance d'internet, comme le rapportait dès vendredi 26 décembre **le site NextInpact**.

Définitivement adoptée le 10 décembre 2013, la LPM vise à encadrer, mais également, au passage, à renforcer les pratiques de surveillance d'internet des services de renseignements français. L'article 20 notamment pérennise un dispositif voté en 2006, de manière temporaire pour faire face à la menace terroriste, sous l'impulsion du ministre de l'intérieur de l'époque, Nicolas Sarkozy.

Ce texte ouvre la possibilité aux services antiterroristes de consulter les *« données de trafic »* sur simple avis d'une personnalité qualifiée *« placée auprès du ministre de l'intérieur »*, le contrôle de la Commission nationale de contrôle des interceptions de sécurité (CNCIS) ne s'effectuant plus qu'*a posteriori*. Il comporte cependant une clause de renouvellement de trois ans, obligeant le gouvernement à régulièrement le reconduire.

© Reuters

Au prétexte de fusionner le dispositif de 2006 et le régime général des écoutes administratives afin de le pérenniser, l'article 20 de la LPM étend tout d'abord les cas permettant de demander la transmission des communications informatiques et de leurs métadonnées. Outre la prévention du terrorisme, sont désormais concernées les recherches liées à *« la sécurité nationale, la sauvegarde des éléments essentiels du potentiel scientifique et économique de la France* (…), *de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous »*. De plus, désormais, ce ne sont plus seulement les agences dépendant du ministère de la défense et de l'intérieur qui ont la possibilité de demander la collecte de données, mais également le ministère de l'économie et toutes ses administrations, comme Tracfin ou les douanes.

Encore plus inquiétant, la loi permet désormais d'obliger les hébergeurs et les fournisseurs d'accès à fournir les données *« en temps réel »* et sur *« sollicitation du réseau »*. Une formulation particulièrement vague, qui peut laisser craindre un dispositif de collecte des données branché directement sur les réseaux. Seule concession du législateur, le texte prévoit que la personnalité qualifiée chargée de valider les demandes d'interception dépendra, à compter du 1er janvier prochain, du premier ministre.

Le décret d'application signé le 24 décembre précise les modalités de nomination de cette *« personnalité qualifiée »*. Celle-ci, ainsi que les adjoints qui lui seront affectés, sera désignée par la CNCIS parmi une liste de noms établie par le premier ministre. Une fois en place, elle sera chargée d'examiner les demandes

d'interception déposées par un service de l'État puis de les transmettre à l'hébergeur ou l'opérateur concerné. Les mises sur écoutes devront être autorisées, pour une durée maximale de 30 jours renouvelable, *« par décision écrite du premier ministre ou des personnes spécialement désignées par lui »*.

Concernant les données pouvant être collectées, le décret les limite aux *« données d'identification »* de l'utilisateur ainsi que les *« métadonnées »*, c'est-à-dire les données d'un fichier permettant de connaître son auteur, sa date de création, de modification, éventuellement à qui il a été envoyé, par qui… Mais on apprend, dans une délibération de la Commission nationale de l'informatique et des libertés (CNIL) datée du 4 décembre et **également récemment publiée au Journal officiel**, que le gouvernement en espérait bien plus. En effet, une première version du décret prévoyait de permettre la collecte des *« informations et documents,* "y compris" *les données limitativement prévues par le cadre juridique en vigueur »*. Mais la CNIL a estimé que *« cette formulation pourrait être interprétée comme permettant un élargissement des données pouvant être requises par rapport à celles pouvant actuellement être demandées aux opérateurs »*.

Finalement, le texte limite *« les informations et documents »* pouvant être collectés, *« à l'exclusion de tout autre »*, à une liste fixée par trois textes : les articles **R10-13** et **R10-14** du Code des postes et des communications électroniques, ainsi qu'à l'article 1er**du décret du 25 février 2011** relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'une contenu mis en ligne. Cette liste comporte, notamment, les identités et adresses d'un abonné, l'identifiant de la connexion, les mots de passe, les dates et heures de connexion, les caractéristiques de la ligne de l'abonné, les adresses internet et comptes associés, les éventuels paiements…

La CNIL est par contre plus sévère concernant la possibilité de *« sollicitation du réseau »« en temps réel »* ouverte par la LPM, une notion encore une fois floue qui avait suscité de nombreuses inquiétudes. Or, souligne la commission, *« les débats parlementaires incitaient à penser que cette disposition se limitait exclusivement à l'utilisation de la géolocalisation »*. Mais, depuis, le Secrétariat général de la défense et de la sécurité nationale (SGDN) a *« infirmé cette position en indiquant qu'il convenait que les dispositions réglementaires ne soient pas figées dans le temps au regard des évolutions technologiques »*. *« Au regard des risques potentiels en matière de protection de la vie privée et de protection des données personnelles »*, poursuit la CNIL, *« la commission ne peut que regretter que le projet de décret ne permette pas de définir précisément et limitativement le périmètre de ce nouveau type de réquisition. »*

Même la CNCIS s'inquiète

Il y a un peu plus d'un an, peu après la promulgation de la LPM, le gendarme des données personnelles avait déjà fait part de ses inquiétudes. **Dans son communiqué**, la CNIL regrettait *« de ne pas avoir été saisie de ces dispositions par le gouvernement lors de l'examen du projet de loi »*. Elle s'inquiétait également *« que le recours à la notion très vague* "d'informations et de documents" *traités ou conservés par les réseaux ou services de communications électroniques, semble permettre aux services de renseignement d'avoir accès aux données de contenu, et non pas seulement aux données de connexion »*. Pour la CNIL, *« une telle extension, réalisée dans le cadre du régime administratif du recueil de données de connexion, risque d'entraîner une atteinte disproportionnée au respect de la vie privée »*.

Dans sa délibération, la CNIL souligne par ailleurs que, même une fois définitivement entrée en vigueur, c'est-à-dire une fois la *« personnalité qualifié »* nommée, la LPM risque de faire l'objet de contestations judiciaires. Au mois d'avril dernier, la Cour de justice de l'Union européenne (CJUE) a invalidé la directive européenne sur les données personnelles, mettant ainsi potentiellement dans l'illégalité le dispositif de la LPM qui prévoit que les données pourront être conservées pour une durée maximale de trois ans. *« Cet arrêt»*, écrit

la CNIL, *« conduit à s'interroger sur le risque d'inconventionnalité des dispositions de la loi de programmation militaire. Au-delà de ce champ d'application spécifique, la commission relève que les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses, sont accessibles à un nombre de plus en plus important d'organismes, sur réquisitions judiciaires ou administratives ou en exécution d'un droit de communication, et ce pour des finalités très différentes. »*

Une autre salve de mises en garde est récemment venue de la CNCIS même, l'autorité chargée de contrôler les demandes d'interception. **Lors de son audition**, à la mi-novembre, par la Commission de réflexion sur le droit et les libertés à l'âge du numérique de l'Assemblée nationale, son nouveau président Jean-Marie Delarue a dressé un état des lieux inquiétant du dispositif de contrôle actuel qui, selon lui, *« n'est pas satisfaisant »*. L'ancien contrôleur général des lieux de privation, nommé à la tête de la CNCIS au mois de juin dernier par François Hollande, a notamment regretté que son institution a été dépossédée de son droit de regard prioritaire au profit de cette *« personnalité qualifiée »*, *« dont les qualités personnelles ne sont pas en doute mais sur l'indépendance de laquelle on peut légitimement s'interroger »*. *« Il a été reconnu en cedomaine le contrôle de la CNCIS»*, précise-t-il, *«mais c'est un contrôle* a posteriori *et c'est la personnalité qui donne toutes les autorisations nécessaires. Je le regrette. »*

Plus généralement, Jean-Marie Delarue s'est inquiété de la banalisation de la collecte des métadonnées à laquelle l'article 20 de la LPM ouvre la voie. Alors que celle-ci est souvent présentée comme plus respectueuse de la vie privée des personnes qu'une mise sur écoute classique, collectées de manière systématique, ces métadonnées sont souvent bien plus intrusives que la simple écoute de communications. De nombreux documents dévoilés par Edward Snowden ont d'ailleurs montré qu'elles faisaient l'objet de campagnes d'interception massives de la part de la NSA et de ses partenaires, parmi lesquels la France. *« Je suis personnellement persuadé que la saisie répétitive et portant sur des domaines étendus de métadonnées révèle autant en matière de contenant que la saisine de certains contenus*, a témoigné Jean-Marie Delarue devant la commission. *Elle révèle d'autant plus que, bien entendu, ceux qui pensent être l'objet d'interceptions de sécurité sont en général discrets dans leurs propos. La saisine de contenant parle beaucoup plus que ce qu'ils peuvent dire au téléphone. »*

Le président de la CNCIS plaide ainsi pour que les métadonnées bénéficient de la même protection que les communications elles-mêmes, et appelle à réformer la loi dans ce sens. *« On a justifié ces différences, entre les interceptions de sécurité et les métadonnées, et donc différences de procédure, en disant : les secondes sont moins intrusives que les premières.* (…) *Cette façon de considérer comme des degrés de moindre intrusion la saisie de métadonnées n'est pas pour moi un très bon calcul. Et par conséquent, les choses doivent évoluer sur ce point*, a-t-il déclaré lors de son audition. *Il faut donner à toute espèce de contrôle des garanties d'indépendance et ces garanties pour moi n'existent pas dans toutes les procédures actuelles. »« Donc, je pense* (…) *que l'évolution de la loi est nécessaire. »*

C'est à une véritable réforme renforçant les droits des citoyens que le nouveau président du CNCIS appelle. *« Notre société est plus sensible au besoin de sécurité.* (…) *Les composantes de la menace se sont modifiées avec une dimension terroriste qui n'existait pas en 1991. La criminalité internationale a renforcé son efficacité si je puis dire. Et puis, comme on le sait, les moyens de communication, je n'ai pas besoin de vous l'apprendre, se sont considérablement développés »*, a expliqué Jean-Marie Delarue. *« Si les données changent, naturellement,* (…) *les services s'adaptent aussi. Et le risque est grand de voir se développer de nouvelles approches plus ou moins intrusives sans dispositions législatives et donc sans les garanties qui entourent les interceptions de sécurité. »*

Directeur de la publication : Edwy Plenel
Directeur éditorial : François Bonnet
Le journal MEDIAPART est édité par la Société Editrice de Mediapart (SAS).
Durée de la société : quatre-vingt-dix-neuf ans à compter du 24 octobre 2007.
Capital social : 28 501,20€.
Immatriculée sous le numéro 500 631 932 RCS PARIS. Numéro de Commission paritaire des publications et agences de presse : 1214Y90071 et 1219Y90071.
Conseil d'administration : François Bonnet, Michel Broué, Gérard Cicurel, Laurent Mauduit, Edwy Plenel (Président), Marie-Hélène Smiéjan, Thierry Wilhelm. Actionnaires directs et indirects : Godefroy Beauvallet, François Bonnet, Laurent Mauduit, Edwy Plenel, Marie-Hélène Smiéjan ; Laurent Chemla, F. Vitrani ; Société Ecofinance, Société Doxa, Société des Amis de Mediapart.

Rédaction et administration : 8 passage Brulon 75012 Paris
Courriel : contact@mediapart.fr
Téléphone : + 33 (0) 1 44 68 99 08
Télécopie : + 33 (0) 1 44 68 01 90
Propriétaire, éditeur, imprimeur : la Société Editrice de Mediapart, Société par actions simplifiée au capital de 28 501,20€, immatriculée sous le numéro 500 631 932 RCS PARIS, dont le siège social est situé au 8 passage Brulon, 75012 Paris.
Abonnement : pour toute information, question ou conseil, le service abonné de Mediapart peut être contacté par courriel à l'adresse : serviceabonnement@mediapart.fr. ou par courrier à l'adresse : Service abonnés Mediapart, 4, rue Saint Hilaire 86000 Poitiers. Vous pouvez également adresser vos courriers à Société Editrice de Mediapart, 8 passage Brulon, 75012 Paris.